Artificial Intelligence Based Mutual Authentication Technique with Four Entities in 4-G Mobile Communications

Pijush Kanti Bhattacharjee
Electronics and Communications Engineering Department,
Bengal Institute of Technology and Management, Santiniketan, Pin-731236, West Bengal, India.
pijushbhatta_6@hotmail.com

***Abstract*—4-G mobile communications system has utilized high speed data communications technology having connectivity to all sorts of networks including 2-G and 3-G mobile networks. Authentication of mobile subscribers and networks are a prime criterion to check and minimize security threats and attacks. An artificial intelligence based mutual authentication system with four entities is proposed. A person talking salutation or greeting words in different times are always consisting of a very narrow range of frequencies which are varying in nature from person to person. Voice frequency of the salutation or selective words used by a subscriber like Hello, Good Morning etc is taken as first entity. Second entity is chosen as frequency of flipping or clapping sound of the calling subscriber. Then third entity is taken as face image of the calling subscriber. Fourth entity is granted as probability of salutation or greeting word from subscriber's talking habit (set of salutation words) while initializing a call. These four entities such as probability of particular range of frequencies for the salutation word, frequency of flipping sound, face image matching of the subscriber, particular salutation or greeting word at the time of starting a call are used with most frequently, more frequently and less frequently by the calling subscriber like uncertainty in Artificial Intelligence (AI). Now different relative grades are assigned for most frequently, more frequently and less frequently used parameters and the grades are modified according to the assumed weightage. A Fuzzy Rule (condition) by Fuzzy operation is invented. If the results obtained from fuzzy operations are satisfied by the fuzzy rule, the subscriber (MS) and the network (Switch or Server) are mutually authenticated in 4-G mobile communications.**

***Index Terms*—Biometric Scheme, Clapping Sound, Flipping Sound, Fuzzy operation, Identifier, Mutual authentication, Packet Switching, Salutation word.**

I. INTRODUCTION

High speed data transmission [1]–[5] in 4-G mobile communications is developed due to the demand of speedy data network and Internet technology. Thus 4-G is invented to integrate a multitude of cellular and wireless networking technologies which include 2nd Generation (2-G), 3rd Generation (3-G) cellular networks with Internet, PSTN (Public Switched Telephone Network), PDN (Public Data Network), ISDN (Integrated Services Digital Network), Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), WCAN (Wireless Corporate Area Network), WHAN (Wireless Home Area Network), WiFi, WiMAX, MANET (Mobile Ad Hoc Network), VANET (Vehicle Ad Hoc Network).

Application of AI on mobile subscriber and network authentication is a new horizon. The particular range of frequency of the salutation (greeting) word, frequency of flipping sound, face image matching, salutation word are used with most frequently, more frequently, less frequently by a calling subscriber while initializing a call. Now different relative grades are assigned for most frequently, more frequently, less frequently used parameters considering talking pattern of the subscriber. Fuzzy sets [3], [5] are derived from the modified relative grades which are obtained by assigning weightage. Then fuzzy operations are performed on fuzzy sets, results of fuzzy operations are analyzed by setting an invented fuzzy rule or condition. If the results are satisfying the fuzzy rule, the subscriber (MS) as well as the network (MSC or PDSN) is authenticated, otherwise not.

II. ARCHITECTURE OF 4-G MOBILE SYSTEM

Architecture of a 4th Generation wireless network is described below in Fig. 1. This 4-G network can provide circuit switched voice service, circuit switched data service like 2-G (CDMA One or GSM), 3-G (WCDMA, CDMA-2000, UMTS) [1]-[3], in addition to this packet switched data and multimedia service at a very high data rate. MS, BTS, BSC, MSC, PSTN, PDN, ISDN, IP Network, AAA Server, Workstations, Gateway etc are functioning same as it is in 2-G or 3-G mobile communications networks.
RNC – Radio Network Controller in UMTS (Universal Mobile Telecommunication Service) in 3-G, 4-G like BSC in GSM or CDMA (2-G and 3-G).

In UMTS (Universal Mobile Telecommunications System) 3-G and 4-G, the core network i.e. server or switch consists of Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) which are interconnected via IP network. The SGSN keeps track the location of individual mobile stations and performs security functions and access control. The GGSN encapsulates packets received from external IP networks and routes them towards the SGSN. GGSN directs outside data to SGSN. SGSN is connected to the Radio Network Controller (RNC) which is further attached to BTS via asynchronous transfer mode; both RNC and BTS

DOI: 01.IJCOM.01.03.43

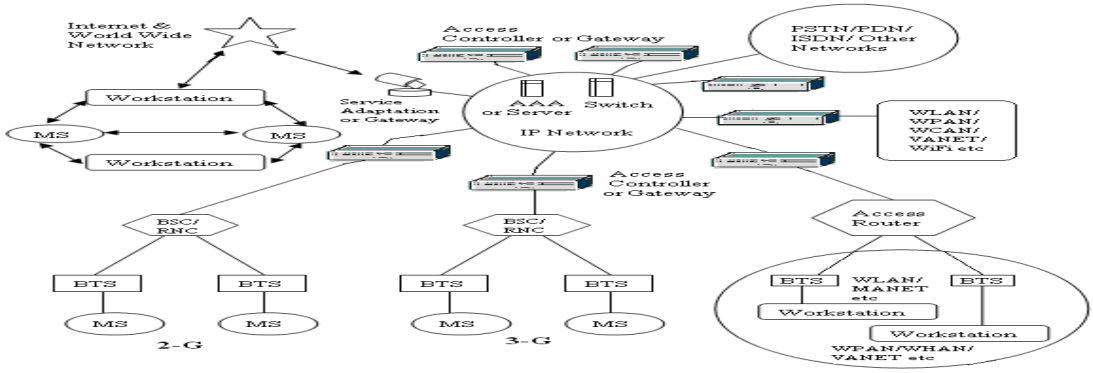

Fig. 1. Wireless Network Architecture for 4th Generation (4-G) Mobile Communications System

stay in UTRAN (UMTS Terrestrial Radio Access Network) unit. RNC is in charge of the overall control of the logical resources provided by UTRAN.

III. PROPOSED ARTIFICIAL INTELLIGENCE BASED AUTHENTICATION TECHNIQUE IN 4-G MOBILE NETWORK

It is having two different phases, namely, Subscriber Enrollment Phase and Subscriber Authentication Phase.

A. Subscriber Enrollment Phase

The subscriber is enrolled to particular server or switch belonging to the network. This phase is executed once.

ASE1: The subscriber sends an application request to the mobile service provider for a new SIM.

ASE2: After receiving the request, the authority asks to submit his different parameters of talking and Flipping or Clapping sound (Biometric attributes) and tests his different talking habit. This flipping or clapping sound is varying in frequency from one subscriber to another subscriber, depends on the subscriber's body parameters.

ASE3: (i) Which frequency range in voices is appearing most frequently, more frequently and less frequently used by the subscriber in talking salutation or greeting words?

(ii) What are most frequently, more frequently and less frequently frequency of the subscriber's flipping sound?

(iii) Which subscriber's face image in the database is most frequently, more frequently and less frequently matched with the calling subscriber's face image?

(iv) Which salutation words are most frequently, more frequently and less frequently used by the calling subscriber at the time of starting a mobile call?

Frequency of salutation word and flipping sound are measured by sophisticated electronics instrument in Hz upto one decimal place and face image of the subscriber is taken by digital camera with high resolution, generally both the instruments may inbuilt in mobile phone (MS).

ASE4: The authority uses above four databases in the sever or switch for storing the subscriber parameters based on talking habit. The first database, D_V stores the subscriber most frequently, more frequently and less frequently used voice frequencies for each salutation word and its corresponding relative grades. The first range of voice frequency for the salutation word, D_{VR1} of D_V, is assigned relative grade by 0.65. The second class D_{VR2} of $D_{V,}$ stores the more frequently used voice frequency of the salutation word having relative grade 0.23. The third range D_{VR3} of $D_{V,}$ less frequently used frequency of the salutation word with relative grade 0.12.

The second database, D_F stores the most probable, more probable and less probable flipping frequency of the subscriber and its relative grades. D_{FR1} of D_F, most frequently (dominant) used frequency of the flipping sound has relative grade 0.9. The second class D_{FR2} of $D_{F,}$ the more frequently used frequency of the flipping sound has relative grade 0.6. The third range D_{FR3} of $D_{F,}$ the less frequently flipping frequency is having relative grade 0.3.

The third database, D_I stores face image of all subscribers with their statistical attributes like mean, standard deviation (std), moments, correlation coefficient, covariance etc or any other attributes like histogram, region, pixel indexing etc in the server or switch of a network e.g. each face image consisting of 16x16 pixels with its statistical or other parameters. First calling subscriber's face image matching is done by comparing statistical parameters of the calling subscriber's face image with that of each stored data base image, accordingly the best match or nearest image is searched out. Then the calling subscriber's image is again compared with the best match image by matching each location pixels i.e. pixel wise. The number of pixels are matched either having same values or thresholding i.e. upto certain range say 10 or 15 or any appropriate value. If the best match face image in the data base to the calling subscriber's face image falls under category of 81% to 100% pixels matching, relative grade is 0.9, stored in D_{IR1}. If 61% to 80% pixels are matched for the best match image, relative grade is 0.8, stored in D_{IR2}. If 41% to 60% pixels are matched, relative grade is 0.3, stored in D_{IR3}. The fourth database, D_W stores the most frequently, more frequently and less frequently used salutation words and their corresponding relative grades. The first row, D_{WR1} of $D_{W,}$ stores the most frequently used salutation words with relative grade 0.9. The second row, D_{WR2} of $D_{W,}$ the more frequently used salutation words with relative grade 0.6. The third row, D_{WR3} of D_W, the less frequently used salutation words with relative grade 0.3.

DOI: 01.IJCOM.01.03.43

Different weightages to these parameters are imposed. $D_V : D_F : D_I : D_W = 1 : 0.9 : 0.8 : 0.75$. The relative grades are to be multiplied by the corresponding weightage for computing the modified relative grades.

ASE5: If the authority does not get sufficient information, request for resubmission correct signature or database of the subscriber is placed. Then the authority executes the above steps again to create a strong database.

B. Subscriber Authentication Phase

When a subscriber intending a call by speaking a salutation word, the authentication process starts. Then the server or switch executes the following operations:

ASA1: Finds the matched frequency of the salutation word within the rows $D_{VR1,}$ D_{VR2}, D_{VR3} of D_V.

ASA1.1: After hearing the first word from a subscriber, either MS or server computes frequency of the salutation word, then match the voice frequency of the salutation word within the stored range $D_{VR1,}$ D_{VR2}, D_{VR3} of D_V and its corresponding relative grade which is taken as v1, If not match, v1 = 0. The membership functions of a fuzzy set F1 can be defined as follows,

μ_{F1} (a1) = v1, [Since, weightage of v1 is 1]

Hence, F1 = {(a1, v1)}

ASA2: Finds the matched flipping frequency within the rows $D_{FR1,}$ D_{FR2}, D_{FR3} of D_F.

ASA2.1: If the flipping frequency of the MS is matched, then stores p1= Relative grade of matched location in row, otherwise p1=0. The modified value of p1 according to the weightage is $p1_{m,}$ where $p1_m = (p1) \times 0.9$,

The membership functions of a fuzzy set F2 is

μ_{F2} (a2) = $p1_m$, Hence, F2 = {(a2, $p1_m$)}

ASA3: Finds the matched subscriber face image within the rows $D_{IR1,}$ D_{IR2}, D_{IR3} of D_I.

ASA3.1: If the face image of the MS (calling subscriber) is compared with the stored best match database image in the server or switch which are obtained by differencing statistical or any other parameters, then stores value

q1= Relative grade of matched location in row, otherwise q1=0. Thus the modified value of q1 according to the weightage is $q1_{m,}$ where $q1_m = (q1) \times 0.8$,

The membership functions of a fuzzy set F3 can be,

μ_{F3} (a3) = $q1_m$, Hence, F3 = {(a3, $q1_m$)}

ASA4: Finds the matched salutation or greeting word within the rows $D_{WR1,}$ D_{WR2}, D_{WR3} of D_W.

ASA4.1: If the salutation word is matched within the stores value of $D_{WR1,}$ D_{WR2}, D_{WR3}, then it stores

w1= Relative grade of the matched salutation word in row, otherwise w1=0. The modified value of w1 according to weightage is $w1_m$, where $w1_m = (w1) \times 0.75$,

The membership functions of a fuzzy set F4 can be,

μ_{F4} (a4) = $w1_m$, Hence, F4 = {(a4, $w1_m$)}

ASA5: Computes fuzzy operations,

ASA5.1: $\mu_{F1 \cap F2 \cap F3 \cap F4}$ (a) = min {μ_{F1} (a1), μ_{F2} (a2), μ_{F3} (a3), μ_{F4} (a4)}

ASA5.2: $\mu_{F1 \cup F2 \cup F3 \cup F4}$ (a) = max {μ_{F1} (a1), μ_{F2} (a2), μ_{F3} (a3), μ_{F4} (a4)}

ASA6: For ascertaining authenticity of the mobile subscriber (MS) as well as the network (MSC or PDSN), an invented Fuzzy Rule (condition) on result of the fuzzy operations has evolved. The Fuzzy Rule is to be obeyed,

If $\mu_{F1 \cap F2 \cap F3 \cap F4}$ (a) $\geq$ 0.22 and

$\mu_{F1 \cup F2 \cup F3 \cup F4}$ (a) $\geq$ 0.65 satisfies, then only the server ensures that the subscriber is authentic, hence their mutual authenticity is verified. Also if the above two fuzzy conditions are not satisfied, the server ensures that the user or the subscriber (MS) is unauthentic. The server sends an authentication failure message to the subscriber.

IV. ADVANTAGES OF THE AUTHENTICATION TECHNIQUE

This technique is the most efficient due to artificial intelligence used and no further information has to be supplied by the subscriber (MS) while making a call. So it is a unique one. Authenticity is decided by the subscriber's talking characteristics (habit) and face image analysis. No cryptography algorithm or any complex functions are applied. This authentication technique enables to offer correct result with in a real time basis.

V. REMARKS

In this proposed 4-G artificial intelligence (AI) based authentication technique, subscriber as well as network mutual authentication scheme is developed. A novel artificial intelligence is introduced to the server for this mutual authentication purpose which works in a real time basis in 4-G mobile communications network.

REFERENCES

[1] William C. Y. Lee, *Wireless and Cellular Communications*, 3rd Edition, McGraw Hill Publishers, 2008.

[2] M. L. Roberts, M. A. Temple, R. F. Mills, and R. A. Raines "Evolution of the Air Interface of Cellular Communications Systems toward 4G Realization", *IEEE Communications Surveys and Tutorials*, vol. 8, no. 1, pp. 2-23, Mar 2006.

[3] C. Koner, P. K. Bhattacharjee, C. T. Bhunia, U Maulik, "A Novel Approach for Authentication Technique in Mobile Communications", *International Journal of Computer Theory and Engineering*, Singapore, vol. 1, no. 3, pp. 225-229, 2009.

[4] H. Kim, H. Afifi, "Improving Mobile Authentication With New AAA Protocols", *IEEE International Conference on Communication (ICC 2003)* vol 1, pp. 497-501, May, 2003.

[5] Vilem Novak, Jiri Mockor, Irina Perfilieva, *Mathematical Principles of Fuzzy Logic*, Kluwer Academic Publisher, 2006.

Dr. Pijush Kanti Bhattacharjee is having qualifications ME, MBA, MDCTech, AMIE, BSc, BA, LLB, BIASM, CMS, PET, EDT, FWT, DATHRY, BMus, KOVID, DH, ACE, FDCI etc. He worked in Department of Telecommunications (DoT), Govt. of India as an Engineer from June 1981 to Jan 2007 (26 years), lastly holding Assistant Director post at RTEC [ER], DoT, Kolkata, India. Thereafter, he works as an Assistant Professor in Electronics and Communication Engineering Department at IMPS College of Engineering and Technology, Malda; Haldia Institute of Technology, Haldia; Bengal Institute of Technology and Management, Santiniketan, WB, India. He has written two books "Telecommunications India" & "Computer". He is a Member of IE, ISTE, IAPQR, IIM, India; CSTA, USA; IACSIT, Singapore and IAENG, Hongkong.

DOI: 01.IJCOM.01.03.43